Checklist for new arrivals at CMM

CMM
Center for Molecular Medicine

Name _____ Title _____

E-mail _____ Phone _____

Group/Team leader (or other with delegated responsibility) _____

Research group _____

CMM L8 access after working hours required for floors _____
(write floor numbers)

Access required to the following locked rooms (e.g. chemical room) _____

Keys required for the following rooms _____

Expiration date (max 5 years) _____ Group/Team leader ZZ-code/KST _____

Mandatory read checklist

☐ CMM GDPR policy[1,2] Date _____

☐ Liability agreement CMM IT[1,2] Date _____

☐ Safety orientation with group leader or safety officer[1,3] Date _____

☐ Completed KI lab safety web test[4] (only KI-ID or student-ID holders) Date _____

☐ CMM introduction document[3] Date _____

☐ Instructions for locked room received[5] Date _____

I have made sure my new group member has received all relevant information and specific instructions regarding his or her work at CMM

Group/Team leader/other responsible Name _____

Signature _____ Date _____

I have read and understood all information regarding my work at CMM

Signature new CMM member _____ Date _____

[1] Mandatory before applying for CMM IT account, keys and key cards
[2] Documents are attached in this form
[3] Documents can be found at CMM website: cmm.ki.se - About CMM - Working at CMM - Useful Documents
[4] Mandatory for all staff working in wet lab. KI Laboratory Safety Test can be found at website KI Staff - Digital tools - Pingpong
[5] Mandatory before receiving access to locked rooms (e.g. chemical-, development-, isotope rooms)

Contingent liability agreement

regarding the use of CMM's and KI's computer, network and system resources.

Owner

All computer resources, computer networks, related equipment and accounts are owned and operated by CMM or KI for use in carrying out all university business. All other use, such as for personal development, is only permitted on the following conditions:

- that it does not disrupt normal usage
- that it does not contravene these regulations
- that it does not conflict with departmental rules, CMM's and KI's regulations, SUNET's rules or prevailing laws

By authorized user in these regulations is meant an employee, student or other person who has been allocated an account or granted authorization to use CMM's and KI's computer, network or system resources.

The following conditions apply to all authorized users:

- Authorization and subsequent access to the related resources are strictly non-transferrable.
- Passwords associated with authorization must be kept secret. See the separate document for further details about password regulations (Data Security on the KI intranet).
- Authorization is limited and will be terminated once the period of employment, the project or equivalent at CMM and KI comes to an end. CMM and KI reserves the right to terminate authorization that has been inactive for more than six months unless agreed otherwise.

The following conditions apply to the use of CMM's and KI's computer, network and system resources:

- Acts of sabotage or disruption to the system or other users, and all hacking or attempted hacking into the system from within or outside CMM and KI, are strictly forbidden.
- All commercial use of CMM's KI's computer resources is strictly forbidden unless otherwise agreed.
- The use of misconfiguration, program errors or other methods to acquire extended system rights or other kind of authorization than that which has been granted by system personnel is strictly forbidden.
- Anyone who detects an error, defect, breach of regulations, irregularity or other such problem shall immediately report it to the system manager.
- No material may be copied or distributed unless it is expressly stated otherwise. Material that is copyright protected may only be copied or distributed with the permission of the copyright owner. KI reserves the right to restrict the use of CMM's and KI's equipment for publishing and distributing material.

Breach of regulations

- System managers are obliged to report all infringements of these regulations and the prevailing laws to the IT department. If there is suspicion of criminal activity, the president is empowered to make arrangements for taking legal action. The subsequent penalties range from exclusion from CMM's and KI's ADP resources to a fine or imprisonment. Certain illegal or illegitimate activity may entail the payment of damages.
- System managers are obliged to sign a declaration of secrecy.
- In order to manage the day-to-day operation of the resources and to ensure compliance with these regulations, system managers are entitled, within their sphere of responsibility, to monitor CMM's and KI's systems and check the contents of traffic, data etc. that is either stored or being transmitted.
- System managers are entitled to prevent access to CMM's and KI's computer, network or system resources should they have grounds to suspect that these regulations are being infringed.

Sensitive or important data?

- Sensitive data or confidential information may not be sent over the network in an unencrypted format.
- Prevailing regulations are available in digital form on KI's webserver.
- CMM's and KI's IT departments have resources and data security personnel that can be consulted for information and advice.
- The KI IT department distributes security information when necessary to the local system managers and at its different departments for further distribution to all department members.

I undertake to keep myself informed about the prevailing regulations governing the use of CMM's and KI's computer systems at any one time and to comply with these regulations in full. By signing the Checklist for new arrivals document, I certify that I have read and understood these regulations. I am also aware that any negligent use of the systems or failure to comply with the instructions of the system managers may mean my being denied access to the computer, network or system resources.

CMM GDPR policy

CMM cares about your privacy. For this reason, we collect and use personal data only as it might be needed for us to deliver to you our products, services, websites and mobile applications (collectively, our "Services"). Your personal data includes information such as:

- Name
- Address
- Telephone number
- Email address
- Other data collected that could directly or indirectly identify you.

Our Privacy Policy is intended to describe to you how and what data we collect, and how and why we use your personal data. It also describes options we provide for you to access, update or otherwise take control of your personal data that we process.

If at any time you have questions about our practices or any of your rights described below, you may email helpdesk@cmm.se

What information do we collect?

We collect information so that we can provide the best possible experience when you utilize our Services. Much of what you likely consider personal data is collected directly from you when you:

1. create an account or purchase any of our Services (ex: billing information, including name, address);
2. request assistance from our customer support team (ex: phone number);
3. complete contact forms or request newsletters or other information from us (ex: email); or
4. participate in contests and surveys, apply for a job, or otherwise participate in activities we promote that might require information about you.

However, we also collect additional information when delivering our Services to you to ensure necessary and optimal performance. These methods of collection may not be as obvious to you, so we wanted to highlight and explain below a bit more about what these might be (as they vary from time to time) and how they work:

Account related information is collected in association with your use of our Services, such as account number, purchases, when products renew or expire, information requests, and customer service requests and notes or details explaining what you asked for and how we responded.

Data about Usage of Services is automatically collected when you use and interact with our Services, including metadata, log files, cookie/device IDs and location information. This information includes specific data about

your interactions with the features, contained within the Services, Internet Protocol (IP) address, the date and time the Services were used, information about devices accessing the Services, including type of device, what operating system is used, device settings, application IDs, unique device identifiers and error data, and some of this data collected might be capable of and be used to approximate your location.

How we utilize information.

We strongly believe in both minimizing the data we collect and limiting its use and purpose to only that for which we have been given permission, (2) as necessary to deliver the Services you purchase or interact with, or (3) as we might be required or permitted for legal compliance or other lawful purposes. These uses include:

Delivering, improving, updating and enhancing the Services we provide to you. We collect various information relating to your purchase, use and/or interactions with our Services. We utilize this information to:

- Improve and optimize the operation and performance of our Services
- Diagnose problems with and identify any security risks, errors, or needed enhancements to the Services
- Detect and prevent fraud and abuse of our Services and systems
- Collecting aggregate statistics about use of the Services
- Understand and analyze how you use our Services and what products and services are most relevant to you.

Often, much of the data collected is aggregated or statistical data about how individuals use our Services, and is not linked to any personal data, but to the extent it is itself personal data, or is linked or linkable to personal data, we treat it accordingly.

Sharing with trusted third parties. We may share your personal data with affiliated companies within our corporate family, with third parties with which we have partnered to allow you to integrate their services into our own Services, and with trusted third party service providers as necessary for them to perform services on our behalf, such as:

- Processing payments
- Conducting contests or surveys
- Performing analysis of our Services and customers demographics
- Communicating with you, such as by way email or survey delivery
- Customer relationship management.

We only share your personal data as necessary for any third party to provide the services as requested or as needed on our behalf. These third parties (and any subcontractors) are subject to strict data processing terms and conditions and are prohibited from utilizing, sharing or retaining your personal data for any purpose other than as they have been specifically contracted for (or without your consent).

Communicating with you. We may contact you directly or through a third party service provider regarding products or services you have signed up or purchased from us, such as necessary to deliver transactional or service related communications. These contacts may include:

- Email
- Text (SMS) messages
- Telephone calls

Transfer of personal data abroad. If you utilize our Services from a country other than the country where our servers are located, your communications with us may result in transferring your personal data across international borders.

Compliance with legal, regulatory and law enforcement requests. We cooperate with government and law enforcement officials and private parties to enforce and comply with the law. We will disclose any information about you to government or law enforcement officials or private parties as we, in our sole discretion, believe necessary or appropriate to respond to claims and legal process (such as subpoena requests), to protect our property and rights or the property and rights of a third party, to protect the safety of the public or any person, or to prevent or stop activity we consider to be illegal or unethical.

To the extent we are legally permitted to do so, we will take reasonable steps to notify you in the event that we are required to provide your personal information to third parties as part of legal process.

Third-party websites. Our website and our mobile applications contain links to third-party websites. We are not responsible for the privacy practices or the content of third-party sites. Please read the privacy policy of any website you visit.

How you can update or delete your data.

Please send an email to helpdesk@cmm.se and we will help you update your data. If you make a request to delete your personal data and that data is necessary for the products or services you have purchased, the request will be honored only to the extent it is no longer necessary for any Services purchased or required for our legitimate business purposes or legal or contractual record keeping requirements.

You may also contact us by one of the methods described in the "Contact Us" section below.

How we secure, store and retain your data.

We follow generally accepted standards to store and protect the personal data we collect, both during transmission and once received and stored, including utilization of encryption where appropriate.
We retain personal data only for as long as necessary to provide the Services you have requested and thereafter for a variety of legitimate legal or business purposes. These might include retention periods:

- mandated by law, contract or similar obligations applicable to our business operations;
- for preserving, resolving, defending or enforcing our legal/contractual rights; or
- needed to maintain adequate and accurate business and financial records.

If you have any questions about the security or retention of your personal data, you can contact us at helpdesk@cmm.se

Age restrictions. Our Services are available for purchase only for those over the age of 18. Our Services are not targeted to, intended to be consumed by or designed to entice individuals under the age of 18. If you know of or have reason to believe anyone under the age of 18 has provided us with any personal data, please contact us.

Changes in our Privacy Policy. We reserve the right to modify this Privacy Policy at any time. If we decide to change our Privacy Policy, we will post those changes to this Privacy Policy and any other places we deem appropriate, so that you are aware of what information we collect, how we use it, and under what circumstances, if any, we disclose it. If we make material changes to this Privacy Policy, we will notify you here, by email, or by means of a notice on our home page, at least thirty (30) days prior to the implementation of the changes.

Data Protection Authority.

If you are a resident of the European Economic Area (EEA) and believe we maintain your personal data subject to the General Data Protection Regulation (GDPR), you may direct questions or complaints to our lead supervisory authority, the Integritetsskydssmyndigheten, as noted below:

https://www.imy.se/
Integritetsskydssmyndigheten
Box 8114
104 20 Stockholm

Contact us.

If you have any questions, concerns or complaints about our Privacy Policy, our practices or our Services, you may contact us by either of the following means:

By email: helpdesk@cmm.se
By Phone: +46 8 712 72 22